Descargar registros desde la administración de registros de Umbrella mediante la CLI de AWS

Contenido

Introducción

Este documento describe cómo descargar registros de Umbrella Log Management usando AWS CLI.

Overview

Una vez que haya configurado su administración de registros en Amazon S3, es posible que desee probar los archivos de registro que se están escribiendo y que se pueden descargar.

Para ello, hemos esbozado un enfoque utilizando la 'Interfaz de línea de comandos AWS' de Amazon

Para obtener métodos alternativos, consulte aquí.

Prerequisites

- Descargue e instale la CLI de AWS desde https://aws.amazon.com/cli/
- Cree su cubeta gestionada de Cisco como se describe aquí
- También puede configurar el registro para utilizar su propio depósito S3, como se describe aquí

Configuración de las credenciales de seguridad en AWS CLI

En la línea de comandos, introduzca:

```
aws configure
```

Se le presentan estas cuatro preguntas. Si ha creado un depósito gestionado de Cisco, los tres

primeros se proporcionaron al crear el depósito. En el caso de los cubos gestionados de Cisco, el 'nombre de región predeterminado' aparece en el nombre del cubo. Por ejemplo, la región para "cisco-managed-us-west-2" es "us-west-2". Para su propia cubeta, la región se establece según la configuración de S3. Para obtener una lista completa de las regiones de Amazon S3, por favor, consulte aquí.

Puede volver a ejecutar esta configuración en cualquier momento y mostrará una versión reducida de sus credenciales, por ejemplo:

ID de clave de acceso de AWS [**********HVBA]:

Clave de acceso secreta de AWS [**********OuFw]:

Nombre de región predeterminado [us-west-2]:

Formato de salida predeterminado [Ninguno]:

Sincronizar el contenido del depósito en la carpeta local

Ingrese este comando y reemplace "yourbucketname" y "prefix" por los detalles de su depósito.

```
aws s3 sync s3://<yourbucketname>/<prefix>/ <your local folder path>
```

El prefijo es opcional para los depósitos propiedad del administrador y obligatorio para los gestionados por Cisco. Por ejemplo:

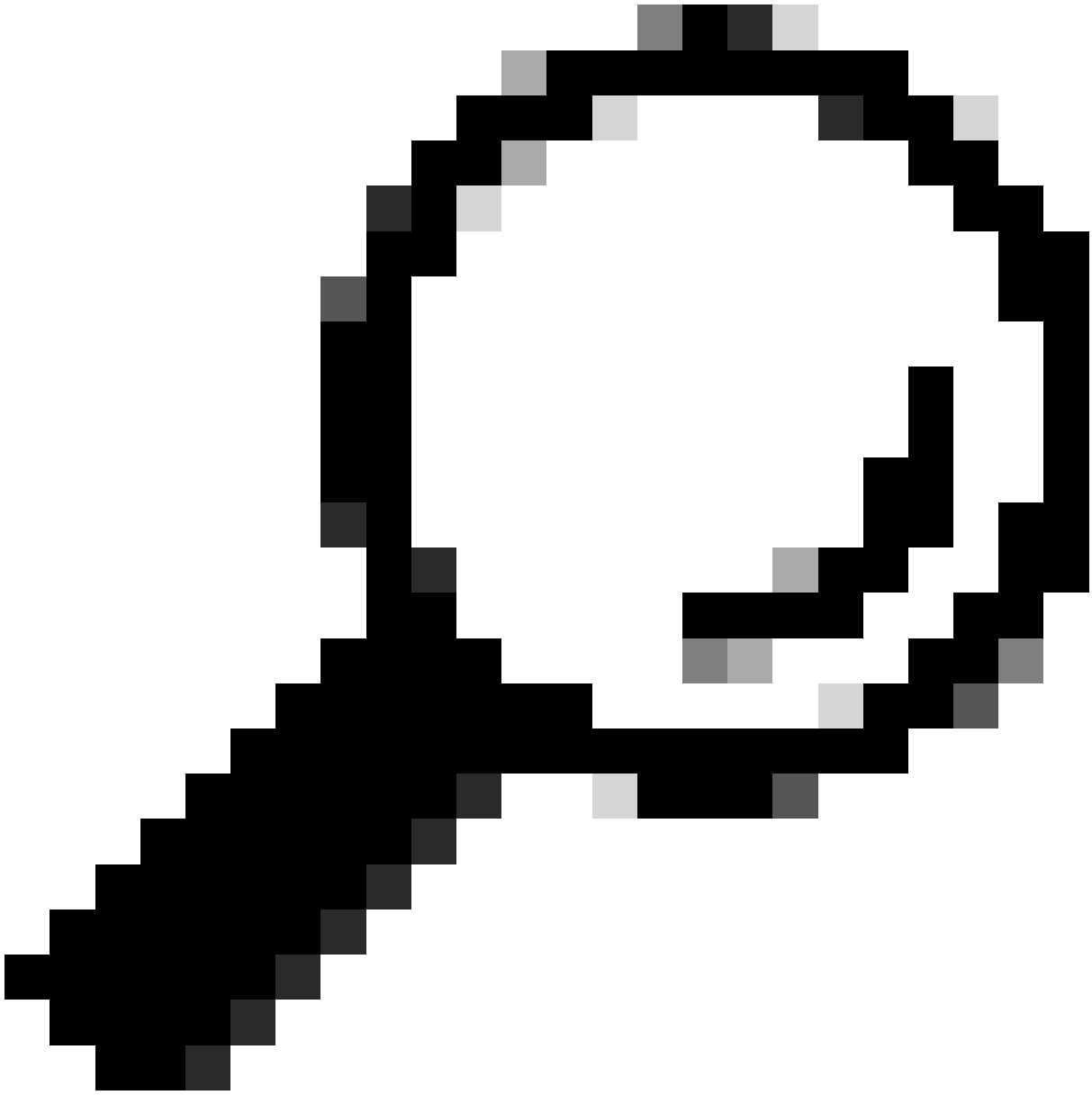
```
aws s3 sync s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/ c:\temp\
```

Puede ver una salida como esta:

descargar: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-30-0e41.csv.gz

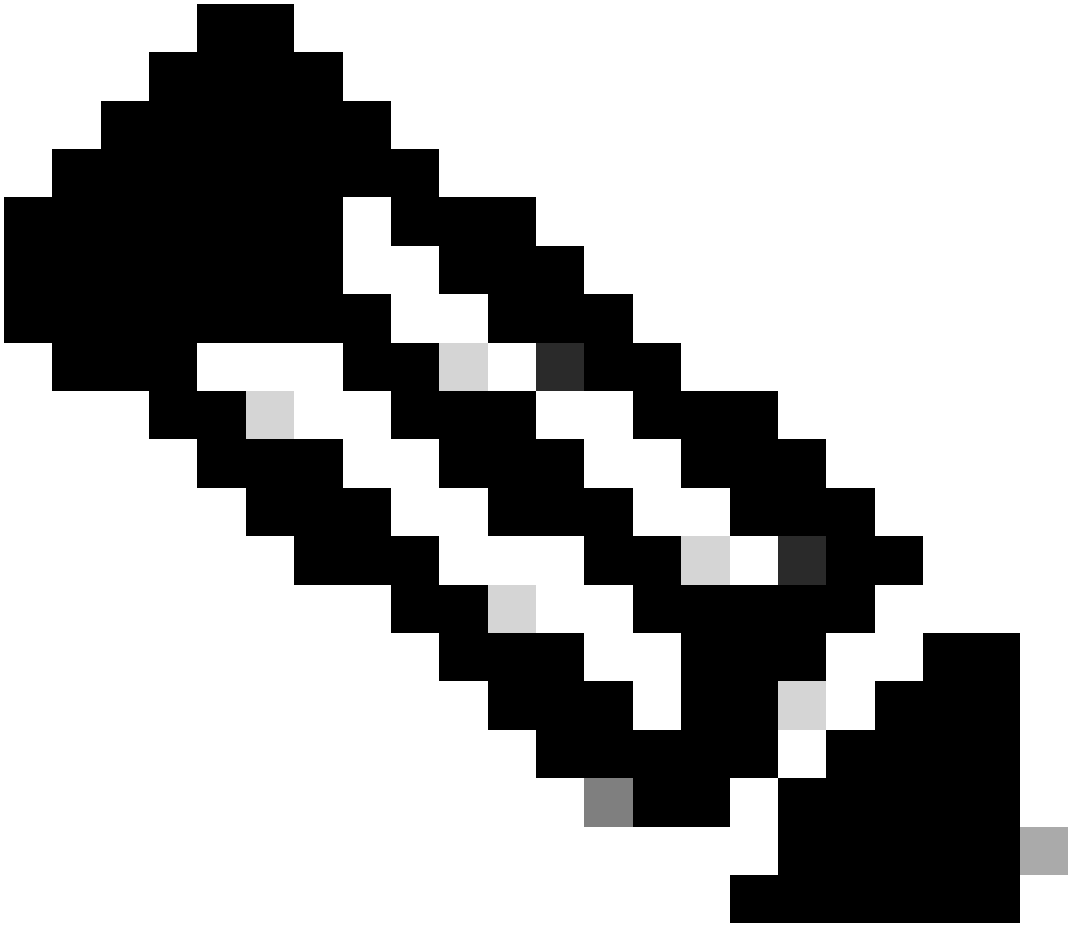
descargar: s3://ccisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-40-0e41.csv.gz to dnslogs\2018-05-01\2018-05-01-12-40-0e41.csv.gz

descargar: s3://cisco-managed-us-west-2/2293370_96b88e0e21ac0136373b7009a340dc5f/dnslogs/2018-05-01/2018-05-01-12-30-b3ab.csv.gz to dnslogs\2018-05-01\2018-05-01-12-30-b3ab.csv.gz



Consejo: Si se intenta enumerar el contenido de una raíz de depósito administrada de Cisco, generalmente se produce un error, ya que el nivel de acceso proporcionado no tiene derechos para enumerar el contenido de la raíz de depósito. Sin embargo, puede enumerar el contenido del prefijo y las carpetas dentro de la cubeta mediante un comando similar a este:

```
aws s3 Is s3:////dnslogs
```



Nota: La documentación completa de la interfaz de línea de comandos está disponible en Amazon aquí.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).